LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Angie Grove

MEMORANDUM

TO:	Legislative Audit Committee Members
FROM:	Kent Rice, Information Systems Audit Manager
CC:	Anna Whiting Sorrell, Director, Department of Public Health and Human Services Ron Baldwin, CIO, Department of Public Health and Human Services
DATE:	October 2012
RE:	Information Systems Audit Follow-up (12SP-26): Combined Healthcare Information and Montana Eligibility System for Medicaid (10DP-07)
ATTACHMENTS:	Original Information Systems Audit Summary

INTRODUCTION

The *Combined Healthcare Information and Montana Eligibility System for Medicaid (10DP-07)* report was issued to the Committee in February 2011 and contains seven recommendations to the Department of Public Health and Human Services (DPHHS). In June 2012, we began gathering preliminary information from DPHHS regarding progress toward implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

CHIMES - Medicaid is the system used by DPHHS to assist staff in making determinations on client eligibility. This audit reviewed various aspects of controls over the system including who has access, how changes are made, how data is entered, and how eligibility is determined. The audit identified areas for improvement including user access, change management, and data integrity. Of the seven recommendations made, three have been implemented, and the other four are being implemented. One area the department is working on is a single sign-on process that will help increase security over access to the system.

BACKGROUND

DPHHS is responsible for managing Medicaid in Montana. One of the responsibilities of DPHHS is determining who is eligible to receive Medicaid coverage. To assist in the administration of Medicaid eligibility, DPHHS contracted with a third-party vendor to develop the Combined Healthcare Information and Montana Eligibility System (CHIMES) - Medicaid. The system was implemented in October 2009 at a cost of approximately $13.4 million. CHIMES - Medicaid is used by eligibility examiners and supervisory staff throughout Montana. The system is designed to process enrollee information entered by eligibility examiners to assist in determining which

Medicaid programs they are eligible for. DPHHS personnel then use the results from the system to make a determination on eligibility.

FOLLOW-UP AUDIT FINDINGS

The following sections summarize progress towards implementing the report recommendations.

Access Management

DPHHS has limited user access based on business need and created a security matrix to manage and monitor user roles. As owners of the data and processes, it is DPHHS' responsibility to grant access and manage security roles. However, we noted access management had been assigned to the system vendor and changes were made that were not reviewed or approved by DPHHS.

Recommendation #1

We recommend the Department of Public Health and Human Services:

A. Reassume management of the system security through role management.
B. Update the Security Matrix to reflect actual role access.

Implementation Status - Being Implemented

Since our audit, the management of system security was transferred from the vendor and assigned to the Human and Community Services Division Security Officer. The Security Officer now has responsibility for managing access roles; however, the vendor still has access to manage roles and the department is not monitoring role changes. As a result, the vendor still has the ability to modify user roles without department knowledge. To address this, DPHHS is currently developing a single sign-on point for CHIMES, which will be completely managed by department security staff. The single sign-on will force any users of department systems, including vendors, to access through a single point. Development of this process is currently in the testing phase. DPHHS anticipated an October 1, 2012 implementation date. DPHHS security staff provided us with an updated Security Matrix indicating it was reviewed and updated March 2011.

Privileged Access

Privileged access allows a user to access screens or processes outside their regular duties or bypass system security or agency policy. We identified one user role within CHIMES - Medicaid that meets the definition of privileged access: the statewide update role. We identified six users assigned this role. The reason for assigning this role is to provide the user with the ability to correct data elements. However, without formal monitoring or review, this level of access increases the risk of users making unapproved changes to client eligibility including adjusting eligibility characteristics to change a client's level of benefits.

Recommendation #2

We recommend the Department of Public Health and Human Services:

A. Document the business need for assigning privileged roles.
B. Establish formal monitoring of activities for all users with privileged access.
C. Ensure segregation exists between users with privileged access and users monitoring role activities.

Implementation Status - Implemented

DPHHS established new policy outlining the business need for assigning privileged access. The policy reiterates that this access is used to modify/correct erroneous files in CHIMES - Medicaid. DPHHS also developed policy directing supervisory personnel not directly responsible for oversight to review the activities of users with privileged access at least twice a year. This policy includes a review by a Bureau Chief and a Division Administrator. The primary reviewer is a Bureau Chief, who has privileged access. However, according to policy, the Bureau Chief's activities are monitored by a Division Administrator who does not have privileged access.

Password Policy

Statewide policy requires passwords be changed by the user at their initial login and be changed at least every 60 days. During the audit, we noted CHIMES - Medicaid does not force users to change passwords at initial login and we identified users who had never changed their password. Further review noted numerous users with passwords older than 60 days.

Recommendation #3

We recommend the Department of Public Health and Human Services strengthen user-level security by ensuring compliance with statewide enterprise password policy.

Implementation Status: Implemented

DPHHS developed formal policy requiring user passwords to be assigned and changed as outlined in state policy. To further enforce this, CHIMES - Medicaid now forces password changes at initial login and produces an error message when a user attempts to login with a password that is older than 60 days.

Access Monitoring

CHIMES - Medicaid has a function to allow security officers to manage user's access. This function could be used to review a user's current access prior to granting further access to ensure conflicting or excessive access is not assigned. It could also be used to ensure access is granted or removed, and to review when the access was changed, and who made the change. During the audit we noted this functionality was not providing effective documentation for use by DPHHS.

Recommendation #4

We recommend the Department of Public Health and Human Services:

A. **Ensure current access information is available to the security officer.**
B. **Ensure documentation accurately depicts when a change occurred and who made the change.**

Implementation Status - Being Implemented

DPHHS requires a security form to be completed and submitted to the Security Officer who must approve it. The Security Officer retains the forms and user information is compiled into a spreadsheet. In addition, the department's network section maintains a system access database that maintains a record of all access requests. The Security Officer completes a six month review of the access list to determine who has access and if the access is still needed. Due to development of the new single sign-on, the Security Officer has not fully completed the six month review, but indicated they have been reviewing roles on an ongoing basis as part of development. According to DPHHS personnel, the new single sign-on will have an action history on the security screens which is not currently available on the system.

Change Control

At the time of the audit, the CHIMES - Medicaid Service Level Agreement between DPHHS and the Statewide Information Technology Services Division (SITSD) required the two organizations to work together to plan and coordinate upgrades and changes. It also required DPHHS to document and test system changes to ensure they perform properly before implementation. Although DPHHS was testing and approving changes, it could not guarantee only approved changes were being implemented because the vendor maintained control of migration to production.

Recommendation #5

We recommend the Department of Public Health and Human Services migrate system changes directly from testing into production.

Implementation Status - Implemented

In response to our recommendation, DPHHS developed procedures instructing the vendor to send updated files to DPHHS who will then instruct SITSD to migrate them into production. This is designed to prevent direct interaction between the vendor and SITSD. In addition, SITSD is expected to notify DPHHS when a change has been migrated. If the vendor were to bypass DPHHS and move files directly to production, this would be reported to DPHHS by SITSD.

Server Security

According to the Service Level Agreement in place at the time of our audit, access to DPHHS systems and databases was to be strictly maintained and only appropriate levels of personnel were to be authorized by DPHHS and SITSD. During our audit, we noted SITSD was using shared usernames and passwords to access CHIMES - Medicaid servers. There is no accountability for data or system changes if nonsecure procedures are used.

Recommendation #6

We recommend the Department of Public Health and Human Services ensure access to system servers is secure.

Implementation Status - Being Implemented

In its response, DPHHS indicated it was working with SITSD to incorporate a process into its service level agreement to ensure access to system servers is secure. However, SITSD no longer uses service level agreements with agencies, and we were unable to identify any new agreement or other document discussing security. According to both SITSD and DPHHS personnel, SITSD uses software to control access to CHIMES servers. Users must log into servers using individual accounts. While this software does log individual user access, it is not currently being used to generate access reports for review by state personnel.

Data Integrity

During our audit, we identified a limited number of data integrity issues, including missing or erroneous data. DPHHS relied on staff and record reviewers to identify issues with data during normal use of the system. We did not identify any continuous testing to identify data anomalies to ensure data integrity.

Recommendation #7

We recommend the Department of Public Health and Human Services strengthen the current process to help identify missing and inaccurate data.

Implementation Status - Being Implemented

According to DPHHS, they are continuing to train staff on system use and policies related to circumstances that could result in data integrity issues. Our review of policy identified several places mentioning required documentation. We noted one example where policy provides information on good cause for not providing specific information. This policy indicates that case notes must be documented. We did not identify any CHIMES reports being used by the department for identifying missing or inaccurate data.

S:\Admin\IS\Follow-up\12SP-26-CHIMES-follow-up-memo.docx/tg